La Question Technique : ça marche comment Internet ? (partie 1/3)

La Question Technique s'intéresse cette fois-ci à Internet, le réseau des réseaux, la Toile, le World Wide Web. Et parce que le sujet est trop vaste pour en faire le tour en un article, ce sont trois "LQT" que nous y consacrerons. Attachez vos ceintures, c'est parti, et on commence avec les bases...

Si vous lisez cette ligne, c'est que vous savez sans doute ce qu'est Internet. Mais connaissez-vous les bases techniques qui ont permis au réseau mondial de révolutionner nos vies en permettant à des milliards d'appareils d'échanger des informations entre eux ?

Le protocole IPv4

Pour faire communiquer autant d'appareils, la première étape est bien entendu de les identifier. C'est le rôle du protocole IP, indissociable d'Internet, au point qu'il en porte même le nom (IP = Internet Protocol). C'est le protocole réseau de plus bas niveau capable de transiter sur Internet, les protocoles de niveau inférieur étant liés à la couche physique de transmission, donc forcément limités à l'échelle locale (par exemple, les protocoles 802.11* pour le Wi-Fi, l'ATM pour l'ADSL…).

Le protocole IPv4 attribue à chaque machine une adresse codée sur 32 bits, qui peut être publique, c'est-à-dire joignable « directement » depuis n'importe quelle machine connectée à Internet ou privée (et donc, utilisée par une seule machine), c'est-à-dire joignable uniquement au sein d'un sous-réseau (utilisable par plusieurs machines dans des sous-réseaux différents).

Les machines peuvent alors échanger des messages, composés d'un bloc de données et d'un en-tête contenant notamment l'adresse source et l'adresse de destination, mais aussi de nombreuses autres informations utilisées pour certaines fonctionnalités d'IPv4.

Le protocole IPv6

Évolution majeure du protocole IP, le protocole IPv6 vise avant tout à augmenter le nombre d'adresses publiques disponibles, en codant les adresses sur 128 bits. IPv4 ne permet en effet de disposer que d'un peu moins de 4 milliards d'adresses IP publiques (2^32 adresses, mais une partie est réservée pour les adresses privées et pour les adresses de début et de fin de sous-réseau), ce qui est aujourd'hui insuffisant. Avec l'IPv6, on passe à 2^128 adresses, soit plusieurs millions de milliards.

Le protocole IPv6 apporte aussi de nombreuses autres évolutions, qui vont permettre de « dépoussiérer » un peu Internet, avec un protocole conçu en prenant en compte de nombreuses contraintes qui avaient été totalement ignorées à l'époque des premières définitions de l'IP, dont les concepteurs n'imaginaient pas forcément qu'il serait utilisé pour un réseau aussi vaste et complexe que l'Internet d'aujourd'hui.

Ces améliorations concernent notamment le routage et de la configuration automatique des adresses, ce qui devrait simplifier la connexion des machines au réseau. Par exemple, une machine peut s'auto-attribuer une adresse IPv6 publique construite à partir de l'adresse de son routeur et de l'adresse matérielle (MAC) de son interface réseau, sans avoir besoin qu'un serveur lui communique une adresse IP.

Comparaison des en-têtes IPv4 et IPv6

Enfin, les en-têtes ont été grandement simplifiés, en supprimant des champs, ce qui devrait améliorer les performances, en réduisant les traitements nécessaires pour construire les en-têtes avant l'envoi des données.

Le routage

Pour acheminer un paquet IP d'une machine à une autre, il faut déterminer le chemin à employer. Comme avec une adresse postale, qui se décompose en pays, région, ville, rue, l'adresse IP (qu'elle soit v4 ou v6) peut être décomposée en sous-réseaux successifs pour localiser le destinataire au sein du réseau.

Pour ce faire, chaque machine connectée à Internet dispose d'une table de routage qui lui permet de déterminer via laquelle de ses interfaces réseau elle doit envoyer le paquet en fonction de l'adresse de destination.

Exemple de table de routage d'une machine connectée à deux réseaux privés, avec deux passerelles vers Internet

Chaque entrée de table de routage contient une adresse IP et un masque qui, ensemble, vont constituer un identifiant de sous-réseau (un sous-réseau est un groupe d'adresse dont les n premiers bits sont identiques), ainsi qu'une adresse d'interface qui indique par quelle interface de la machine ce sous-réseau est joignable et une métrique qui est un indicateur de « longueur » du chemin (ce qui permet d'indiquer un chemin à privilégier quand il y a plusieurs chemins possible : c'est la métrique la

plus faible qui sera utilisée en premier). Si le sous-réseau n'est pas joignable directement, l'entrée de la table de routage contient également l'adresse de la passerelle, qui est une machine appartenant à un sous-réseau directement joignable et qui peut servir de relais pour envoyer un message vers un sous-réseau non joignable.

Par exemple, dans la capture ci-dessus, la ligne « 192.168.84.0 255.255.255.0 On-link 192.168.84.3 276 » indique que toutes les machines dont l'adresse commence par 192.168.84 sont accessibles directement en passant par l'interface réseau dont l'adresse est 192.168.84.3, tandis que la ligne « 0.0.0.0 0.0.0.0 192.168.85.254 192.168.85.3 20 » indique que toutes les adresse ne correspondant pas à un sous-réseau listé dans la table (en l'occurrence, toutes les adresses distantes) doivent passer par la passerelle 192.168.85.254, qui est accessible via l'interface 192.168.85.3 (une autre route est possible via la passerelle 192.168.84.254, mais sa métrique est supérieure).

Un client ou un serveur connecté à Internet a en général une table de routage très simple, qui se limite bien souvent à envoyer toutes les adresses vers une même passerelle. Les tables de routage des routeurs sont par contre bien plus complexes, chaque routeur disposant de nombreuses interfaces pouvant être utilisées pour joindre divers sous réseau.

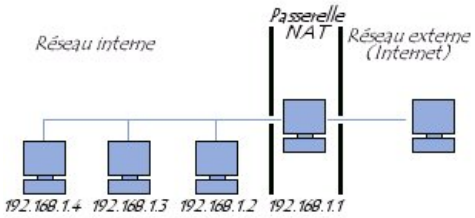
Ces tables sont tellement complexes qu'elles ne peuvent pas être définies à la main, d'autant plus qu'elles doivent évoluer dynamiquement au fil des changements de topologie du réseau (perte d'une connexion, ajout d'une nouvelle connexion…). Plusieurs protocoles ont donc été définis pour permettre aux routeurs de communiquer entre eux et de remplir automatiquement ces tables. Les deux plus utilisés sont OSPF pour la communication entre les routeurs d'un même système autonome (AS, Autonomous System, un ensemble de sous-réseaux cohérents gérés par une même entité, par exemple l'ensemble des sous-réseaux d'un opérateur ou d'une grande entreprise) et BGP pour la communication entre les routeurs d'interconnectant les AS, afin que chaque routeur puisse informer ses « voisins » de la liste des sous-réseaux qu'il gère.

Prefix	Description
2a01:c910::/32	Orange Business Services
2a01:c910:8002::/48	Orange Business Services
2a01:c910:8005::/48	Orange Business Services
2a01:c910:8006::/48	Orange Business Services
2a01:c911::/32	Orange Business Services
2a01:c916::/32	Orange Business Services
2a01:c916::/48	Infra DIH CLB
2a01:c916:0001::/48	Infra DIH MSR
2a01:cb00::/30	Orange S.A.
2a01:cb04::/30	Orange S.A.
2a01:cb08::/30	Orange S.A.
2a01:cb0c::/30	Orange S.A.
2a01:cb10::/30	Orange S.A.
2a01:cb14::/30	Orange S.A.
2a01:cb18::/30	Orange S.A.
2a01:cb1c::/30	Orange S.A.

Liste des sous-réseaux de l'AS3215

Le routage NAT

Comme indiqué plus haut, l'adresse IP dont dispose une machine peut être privée ou publique. Lorsqu'une machine n'a pas d'IP publique, les paquets qu'elle envoie contiennent donc son IP privée comme émetteur, et le destinataire ne pourra donc pas envoyer la réponse. C'est là qu'intervient le routage NAT (Network Address Translation), qui est effectuée par la passerelle. Celle-ci va alors remplacer l'adresse d'émetteur par son adresse publique et mémoriser l'adresse privée associée à la connexion. La réponse sera alors adressée à l'IP publique de la passerelle, qui effectuera alors la translation inverse, en remplaçant cette fois l'adresse de destinataire par l'adresse privée du destinataire pour lui faire suivre la réponse.



La translation peut également s'effectuer sur une requête entrante. Dans ce cas, le choix de l'IP privée vers laquelle sera redirigée la requête entrante se fait en général en fonction du port sur lequel est arrivée la requête ou de manière statique en renvoyant toutes les requêtes vers une même machine (DMZ).

Indispensable en IPv4 (il n'y a pas assez d'adresses publiques pour que tous les appareils puissent en avoir une), le NAT est normalement transparent, mais il peut toutefois poser problème dans certains cas, par exemple avec le protocole FTP en mode actif, qui nécessite l'ouverture d'une connexion dans chaque sens, ou encore lorsque les machines échangent des messages contenant leur adresse IP dans la section de données (la translation ne se fait que sur l'en-tête IP, le destinataire recevra alors un paquet contenant l'IP privée de l'expéditeur).

Bien qu'il puisse en théorie aussi s'utiliser en IPv6, le NAT devrait toutefois disparaitre petit à petit, puisque le nombre d'adresse IP publiques sera largement suffisant pour en attribuer une à chaque appareil connecté.

La couche de transport

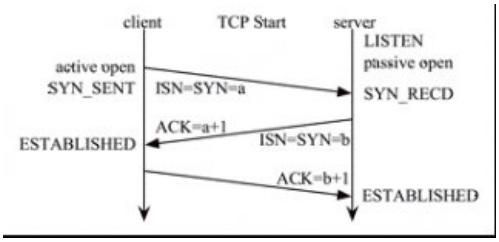
Le protocole IP a été conçu pour ne fournir que le strict minimum nécessaire pour assurer la communication entre deux machines interconnectées. Mais pour de nombreux usages, ce minimum est insuffisant. Le protocole IP ne permet en effet pas d'assurer la validité des données transmises, ni même de garantir qu'elles ont bien été transmises, et les aléas du routage et de la congestion du réseau font que les données n'arrivent pas forcément dans l'ordre dans lequel elles ont été émises. Le protocole IP ne permet par ailleurs pas une identification « fine » du destinataire d'un paquet. Impossible donc d'indiquer au niveau IP qu'un paquet est destiné au serveur FTP d'une machine plutôt qu'à son serveur HTTP.

Divers protocoles dits « de transport » viennent donc se superposer au-dessus du protocole IP pour combler tout ou partie de ces manques. Les deux plus utilisés sont UDP et TCP.

Ces deux protocoles partagent le principe de l'affectation à chaque machine d'un certain nombre de ports de communication (numérotés de 1 à 65535) qui permettent d'identifier le destinataire et l'émetteur d'un paquet au sein d'une machine. Par exemple, un serveur HTTP se mettra généralement en écoute TCP sur le port 80 et recevra donc tous les paquets TCP envoyés à la machine et portant le numéro de port 80. Sur le même principe, une requête sortante émise par une application contient un port de sortie, qui sera repris dans la réponse de la machine distante, ce qui permettra à la réponse d'arriver à la bonne application sur la machine source.

TCP et UDP intègrent également tous les deux un système de somme de contrôle qui permet au destinataire d'un paquet de vérifier que son contenu est bien conforme à ce qui a été envoyé par l'expéditeur.

Le protocole TCP ajoute en plus une notion de session (avant d'échanger les données, les deux machines doivent se « saluer » et échanger divers paquets de contrôle qui vont permettre d'établir une session), une numérotation des paquets, pour que le destinataire puisse les remettre dans l'ordre, des accusés de réception (ACK) permettant à l'expéditeur de vérifier que le destinataire à bien reçu les paquets (avec une possibilité de réémission en cas de perte).



La « poignée de main » TCP, qui permet d'initier la session avant l'envoi de données

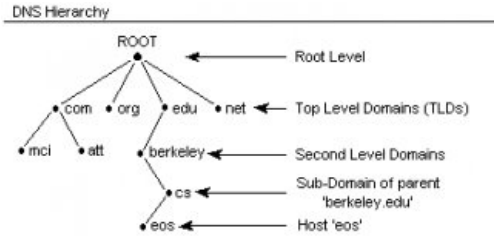
Il intègre également divers mécanismes de contrôle de flux et de contrôle de congestion pour adapter les échanges à la qualité du réseau, par exemple en temporisant les émissions suivantes lorsque les accusés de réception mettent longtemps à arriver ou au contraire en réduisant progressivement les contrôles tant qu'aucune erreur ne survient, pour réduire le surcoût en ressources induit par ces contrôles.

Le choix entre UDP et TCP dépend en général du type d'application qui va être utilisée. Si les performances sont plus importantes que l'intégrité des données, par exemple dans le cas d'un flux de téléphonie IP, où une perte de paquet ou une légère altération est quasiment insensible à l'oreille, c'est l'UDP qui est privilégié, tandis que quand l'intégrité est primordiale, par exemple pour du transfert de fichier, c'est TCP qui est privilégié. Certains protocoles applicatifs coupent également la poire en deux en implémentant leurs propres mécanismes de contrôles d'intégrité.

Le DNS

Maintenant qu'on a l'adressage, le routage et le transport, tout le nécessaire est en place pour permettre à des machines de communiquer entre elles. Mais devant les machines, il y a des hommes, qui ne trouvent pas forcément très pratiques les adresses IP, vides de sens… Il faut donc un système permettant d'attribuer un identifiant un peu plus « user-friendly » aux machines connectées au réseau.

C'est le rôle du DNS (Domain Name System). C'est grâce à lui que vous arrivez sur ce site en tapant www.pcworld.fr dans votre navigateur plutôt que 178.33.22.98. Les adresses DNS sont donc des chaînes de caractères, qui peuvent être choisies presque librement, les seules contraintes étant de respecter un certain jeu de caractères (qui s'élargit petit à petit, par exemple avec l'autorisation des caractères accentués depuis quelques années) et une certaine structure hiérarchique, qui se lit de la droite vers la gauche, les éléments étant séparés par des points.



L'élément le plus à droite est le TLD (Top Level Domain), qui peut être soit ccTLD (country code), comme le .fr, soit un gTLD (genric), comme le .com ou le .info. Au niveau du protocole DNS, le TLD est totalement libre, mais en pratique le système DNS mondial n'autorise qu'une liste bien précise, définie par l'ICANN et régulièrement complétée. Des systèmes DNS alternatifs (notamment les DNS à usage interne en entreprises) peuvent utiliser d'autres TLD.

Le second élément est le domaine de second niveau, souvent appelé simplement domaine. La plupart des gestionnaires de TLD (par exemple l'AFNIC pour le .fr) mettent en ventes les domaines, qui peuvent être choisis librement.

Le domaine peut enfin être précédé d'un ou plusieurs niveaux de sous-domaines, administrés par le propriétaire du domaine.

Lorsqu'une machine doit contacter une autre machine en connaissant son adresse DNS, elle va effectuer une résolution DNS, en contactant un serveur DNS, qui va lui envoyer l'adresse IP correspondant au nom DNS

Notez que la résolution DNS n'est ni injective ni surjective : un même nom DNS peut renvoyer vers plusieurs adresses IP (pour faire de la répartition de charge entre plusieurs machines) et une même adresse IP peut correspondre à plusieurs noms DNS (par exemple, materiel.be et matbe.com pointent tous deux vers la même adresse IP). Dans le cas où plusieurs adresses IP correspondant à un même nom, le serveur va changer l'ordre des adresses à chaque nouvelle requête vers ce nom, pour que la répartition de charge se fasse, sachant que la plupart des clients choisiront systématiquement la première adresse de la réponse.

Comme il y a énormément d'adresses DNS et comme elles changent souvent (création de nouveaux sites, changement d'adresse IP d'un site existant), une architecture distribuée a été mise en place,

pour que chaque serveur DNS n'ait pas à connaître l'intégralité de l'annuaire.

Chaque domaine de second niveau est associé à un ou plusieurs serveurs DNS à qui sont confiés la gestion de la zone DNS (le domaine de second niveau et l'ensemble de ses sous-domaines). C'est ce serveur qui va servir de référence pour faire la correspondance entre tous les noms de la zone et leur adresse IP.

Lorsqu'un client émet une requête DNS vers son serveur DNS, ce dernier va commencer par interroger un des 13 serveurs racines du DNS pour connaître l'adresse d'un serveur DNS gérant le TLD du nom à résoudre, puis il va demander à ce serveur l'adresse d'un serveur DNS gérant le domaine du nom à résoudre, et ainsi de suite jusqu'à arriver sur un serveur DNS capable d'identifier le nom complet. Pour limiter la charge sur les principaux serveurs, toutes les réponses sont mises en cache pour une certaine durée (y compris le client final), fixée par le serveur émettant la réponse.

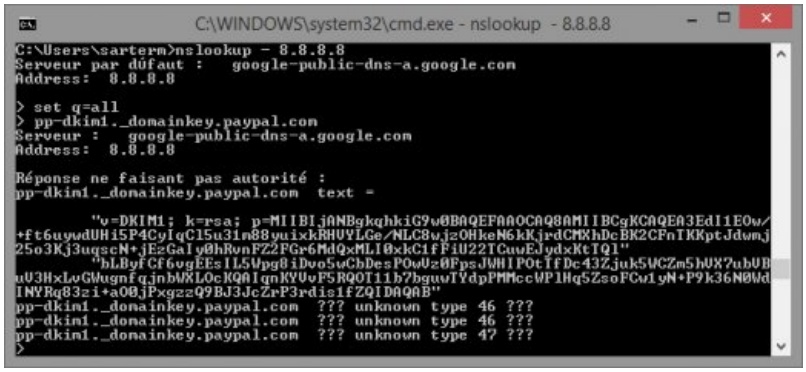
Souvent, les requêtes DNS passent également par des serveurs DNS proxy, qui ne servent que de relais avec cache, pour soulager l'ensemble du système, mais aussi pour accélérer les réponses.

Par exemple, les box Internet intègrent souvent un tel proxy. Lorsque deux ordinateurs situés derrière une même box se connectent successivement à un même site, la requête DNS ne sera donc envoyée qu'une fois vers le serveur proxy DNS du FAI, la seconde occurrence étant servie par le cache de la box.

En cas de mise à jour de l'adresse IP associée à un site, il y a donc un certain délai de propagation avant que tout le monde puisse accéder au site via sa nouvelle adresse, le temps que tous les caches soient mis à jour. C'est pour cette raison que la durée de conservation en cache est fixée par les serveurs qui élaborent les réponses, et non par les clients qui mettent ces réponses en cache. En effet, c'est l'administrateur de la zone DNS qui est le mieux placé pour savoir quelle durée de mise en cache est appropriée à sa zone, cette durée pouvant grandement varier selon les cas…

S'il s'agit d'une zone très stable, où les noms ne changent d'IP que de manière exceptionnelle, la durée de vie d'une réponse (TTL) peut être fixée à plusieurs heures, pour réduire la charge sur le serveur DNS de la zone, alors qu'à l'inverse, dans le cas d'un service de DNS dynamique, comme DynDNS ou No-IP, qui sert à fournir des noms DNS à des machines changeant fréquemment d'IP, il faut une durée de cache très courte, qui tombe parfois à seulement quelques secondes, pour que la nouvelle IP soit prise en compte rapidement.

Outre la résolution de l'adresse IP associée à un nom DNS, le système DNS est également utilisé pour fournir d'autres informations associées au domaine, comme l'adresse des serveurs gérant les adresses mail du domaine (enregistrement MX), qui peuvent être une machine extérieure au domaine (par exemple, le serveur qui gère les adresse mail @pcworld.fr est mail.comparhaut.com), ou encore pour les clés publiques DKIM, qui servent à authentifier les mails dans le cadre de la lutte contre le spam et le phishing.



Exemple d'entrée DNS contenant une clé DKIM

Voilà pour cette première partie consacrée aux bases techniques du réseau et d'Internet. Dans la seconde partie, nous aborderons les protocoles applicatifs (HTTP, FTP...), avant de nous intéresser pour finir aux aspects plus "commerciaux", comme les relations qu'entretiennent les FAI, les problématiques liées au peering, etc. Tout un programme...

Sur le même thème

+ La Question Technique : ARM contre x86, quelles différences fondamentales ?

+ La Question Technique : comment fonctionne la recharge sans fil ?

COMMENTAIRES

Lire les 3 commentaires

VOTRE COMMENTAIRE

suivre ce fil de discussion

Votre commentaire...

Identifiez-vous ou **inscrivez-vous** pour commenter.

Publié le 12 juillet 2014 - Par Matthieu Sarter

3 commentaires

PARTAGER

Partager Tweeter Partager Partager

Connexion Inscription

POUR NOUS SUIVRE...

PCWorld.fr sur Facebook PCWorld.fr sur Google+ PCWorld.fr sur Twitter

newsletter votre@email.com ok

ACTUALITÉS

PCWorld Macworld

samedi 12 juillet

10:00 • LQT : ça marche comment Internet ?

vendredi 11 juillet

17:21 • Asus pense aux gamers, MSI aux écolos
17:03 • **Test : The Wolf Among Us Saison 1**
16:19 • Test : Robot Bluetooth BeeWi
16:07 • **Test : Zotac Zbox Sphere OI520**
15:35 • La Hadopi accélère le rythme
14:41 • Des ROMs alternatives pour Android Wear
14:06 • Free condamné pour tromperie
13:32 • TSMC livre les premiers Apple A8
13:05 • Google : $100 millions pour les startups
12:25 • iWatch : en retard pour Noël
12:09 • Amazon : le feu vert pour ses drones ?
11:19 • Assassin's Creed Pirates offert
11:05 • Les chipsets Série 7 en pré-retraite
10:31 • Watch_Dogs booste les ventes d'Ubisoft
10:13 • Un retour haptique pour le futur iPhone
09:49 • IBM : $3 milliards dans le CPU de demain
09:10 • La parité dans la tech, c'est pas ça !
09:02 • iTunes 11.3 : des bonus pour les fims

jeudi 10 juillet

17:24 • Un smartphone ? Non, un véritable PC !
17:00 • Un kickstarter pour le nouveau Cuisset

16:32 • Pas de nouveaux Mac avant 2015
15:54 • Quid de la fin de support de Windows 7 ?
15:05 • Un nouvel outil pour Google Maps
14:30 • LG : écrans enroulables et transparents
13:41 • Les Google Glass et le contrôle mental
12:57 • Dragon Age 3 : la démo de l'E3
12:33 • La coque arrière de l'iPhone 6
12:07 • Grim Fandango : le remake aussi sur PC
11:27 • Livres Amazon : c'est plus cher !
11:22 • Yosemite adopté plus rapidement
11:00 • Et le premier jeu Android Wear est...
10:15 • Chromecast : le mirroring disponible
10:12 • Panic conçoit une pointeuse iBeacon
09:32 • Un cadre numérique, connecté, et beau
09:06 • Mac : des ventes en légère baisse

mercredi 9 juillet

17:18 • Des photographies des ondes WiFi...
16:50 • Une idée des icônes sous Yosemite
16:38 • Mediatek : du 64 bits en approche
15:48 • Une image du casque de VR Samsung
15:14 • Le créateur d'Alone in the Dark revient
14:22 • KizOn, bracelet connecté pour enfants
13:53 • La boutique refurb d'Apple sur eBay
13:28 • Accord Intel / Panasonic sur le 14 nm
12:40 • iTunes U 2.0 sur iPhone et iPad
12:03 • Brésil - Allemagne : un match record
11:43 • Une batterie trois fois plus endurante
11:38 • Apple embauche deux ingénieurs de Nike
10:59 • Humble 2K Bundle : la bonne affaire
10:30 • iCloud utilise la cartographie Apple

Nous suivre :

Notre réseau :
News Mac, iPad & iPhone - Prix informatique - Comparateur de prix - Prix Electroménager
Nos partenaires :
PCWorld Roumanie

ComparHaut SARL © 2000-2014 | Tous droits réservés à propos | conditions d'utilisation | contact